

日 本 国 特 許 庁  
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日

Date of Application:

2 0 0 4 年 4 月 8 日

出 願 番 号

Application Number:

特 願 2 0 0 4 - 1 1 4 3 3 0

パリ条約による外国への出願  
に用いる優先権の主張の基礎  
となる出願の国コードと出願  
番号

The country code and number  
of your priority application,  
to be used for filing abroad  
under the Paris Convention, is

J P 2 0 0 4 - 1 1 4 3 3 0

出 願 人

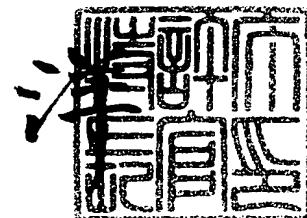
Applicant(s):

松下電器産業株式会社

2 0 0 5 年 4 月 2 0 日

特許庁長官  
Commissioner,  
Japan Patent Office

小 川



BEST AVAILABLE COPY

【書類名】	付託書
【整理番号】	2968260006
【あて先】	特許庁長官 殿
【国際特許分類】	G06K 15/00
【発明者】	
【住所又は居所】	広島県東広島市鏡山3丁目10番18号 株式会社松下電器情報システム広島研究所内
【氏名】	江原 裕美
【発明者】	
【住所又は居所】	広島県東広島市鏡山3丁目10番18号 株式会社松下電器情報システム広島研究所内
【氏名】	植田 栄治
【特許出願人】	
【識別番号】	000005821
【氏名又は名称】	松下電器産業株式会社
【代理人】	
【識別番号】	100105175
【弁理士】	
【氏名又は名称】	山広 宗則
【電話番号】	082-222-9109
【選任した代理人】	
【識別番号】	100105197
【弁理士】	
【氏名又は名称】	岩本 牧子
【手数料の表示】	
【予納台帳番号】	043775
【納付金額】	16,000円
【提出物件の目録】	
【物件名】	特許請求の範囲 1
【物件名】	明細書 1
【物件名】	図面 1
【物件名】	要約書 1
【包括委任状番号】	0215016

【請求項 1】

複数のサービスを提供可能な半導体メモリカードにおいて、

複数のサービス間に共通であり、各サービスのセキュリティレベルを定義したセキュリティレベル情報を設定管理するセキュリティレベル情報管理手段と、

前記セキュリティレベル情報を取得するセキュリティレベル情報取得手段と、

を備えたことを特徴とする、半導体メモリカード。

【請求項 2】

前記セキュリティレベル情報取得手段により取得した、前記セキュリティレベル情報を出力するセキュリティレベル情報出力手段と、

をさらに備えたことを特徴とする、請求項 1 記載の半導体メモリカード。

【請求項 3】

前記セキュリティレベル情報取得手段で取得した前記セキュリティレベル情報を比較するセキュリティレベル情報比較手段と、

前記セキュリティレベル情報比較手段で比較した結果を基に、所定のデータ操作処理を行うデータ操作手段と、

をさらに備えたことを特徴とする、請求項 1 記載の半導体メモリカード。

【請求項 4】

前記セキュリティレベル情報は、前記サービスにおいて取り扱うデータに対する暗号化条件であることを特徴とする、請求項 1 記載の半導体メモリカード。

【請求項 5】

前記セキュリティレベル情報は、前記サービスを提供するアプリケーションのバージョン番号を含むことを特徴とする、請求項 1 記載の半導体メモリカード。

【請求項 6】

前記セキュリティレベル情報比較手段は、さらに、比較結果を保存し、

前記セキュリティレベル情報取得手段は、前記保存されたセキュリティレベル情報が存在する場合、該セキュリティレベル情報を取得することを特徴とする、請求項 1 記載の半導体メモリカード

【請求項 7】

複数のサービスを提供可能な半導体メモリカードに格納されたデータを処理する方法であって、

複数のサービス間に共通であり、各サービスのセキュリティレベルを定義したセキュリティレベル情報を設定管理し、

前記セキュリティレベル情報を取得することを特徴とする、半導体メモリカード処理方法。

【請求項 8】

複数のサービスを提供可能な半導体メモリカードにおいて、該半導体メモリカード内部の CPU により実行される制御プログラムであって、

複数のサービス間に共通であり、各サービスのセキュリティレベルを定義したセキュリティレベル情報を設定管理し、

前記セキュリティレベル情報を取得することを特徴とする、半導体メモリカード処理プログラム。

【請求項 9】

複数のサービスを提供可能な半導体メモリカードにおいて用いられる、集積回路であって、

複数のサービス間に共通であり、各サービスのセキュリティレベルを定義したセキュリティレベル情報を設定管理するセキュリティレベル情報管理手段と、

前記セキュリティレベル情報を取得するセキュリティレベル情報取得手段とを備えること特徴とする集積回路。

【発明の名称】 半導体メモリカード、半導体メモリカード処理方法、半導体メモリカード処理プログラム、および集積回路

【技術分野】

【０００１】

本発明は複数のサービスを搭載可能な半導体メモリカードに関し、特に格納内容のセキュリティを保証し、情報の漏洩を防ぐ事を目的とした半導体メモリカード、半導体メモリカード処理方法及び半導体メモリカード処理プログラム、および集積回路に関するものである。

【背景技術】

【０００２】

現在半導体メモリカードはマスメディアや金融機関、国、自治体など様々な分野から注目を集めている。その理由として、格納データの保護機能が挙げられる。格納データの保護機能を持った半導体メモリカードの代表としてＳＤメモリカードやＩＣカードがある。

図２は一般的なＩＣカードの内部構造を示す図である。従来、クレジットカードをはじめ多くの磁気カードがＩＣカードへ転換されてきている。その理由として、ＩＣカードは半導体メモリを備えるカードであり、プログラムを格納するＲＯＭ２０３、プログラム実行の際に用いられるデータを一時的に格納するＲＡＭ２０２、ＲＯＭ２０３に記憶されたプログラムに従って各種コマンド処理等の制御処理を行うＣＰＵ２０１、外部からダウンロードされたプログラムを格納する書き換え可能なＥＥＰＲＯＭ２０４で構成されている。ＩＣカードは磁気カードに比べて記憶容量が大きいことはもとより、格納される個人情報等のセキュリティ機能の向上がなされていることが特徴として挙げられる。

【０００３】

ところで、このＩＣカードは通常一枚のカード内に電子マネー等の単一のサービスのみを備えて用いられてきたが、近年のＩＣカードにおけるメモリの記憶容量やＣＰＵの処理速度向上にともない、複数のサービスを一枚のＩＣカードで実現するものが提案されてきている。これにより、利用者が複数枚の異なるＩＣカードを所持する必要をなくし、一枚のＩＣカードで異なる様々なサービスを享受することが可能となってきた。

このように、複数のサービスに対応するＩＣカードは、複数のアプリケーションを備えているので、該ＩＣカードを以後マルチアプリケーション対応のＩＣカードと呼び、以後の説明において、単にＩＣカードを示す場合はマルチアプリケーション対応のＩＣカードを意味するものとする。

【０００４】

図３は、上述したＩＣカードにおけるソフトウェア構成を示す図である。ＩＣカードのソフトウェアはレイヤ構造をもち、このレイヤ構造では最下位層にアプリケーション用メモリ領域３１０があり、この上位層にＯＳ３１１、最上位層に複数のアプリケーションが存在し、例えばクライアントＥＣアプリケーション３０１、クライアントＥＣアプリケーション３０２あるいはクライアント公共アプリケーション３０３がある。一般のＩＣカードで複数のサービスに対応するためには、上記のごとく一枚のＩＣカードに複数のアプリケーションを備え、かつ各アプリケーションはＯＳ３１１のファイウォール機能により、互いのアプリケーション用メモリ領域３１０を侵害することはないようになっている。また、従来これらのアプリケーションは互いに独立しており、連携する手段も存在していない。

そのため、例えば、ある電子マネーサービスが保持している電子マネーをサービス提供会社が異なる交通系サービスの電子マネーに移行する場合など、カード外のホスト端末のアプリケーションによりホストにデータを読み出し、ホスト側において、他のアプリケーション等を仲介してデータ交換の可否決定と実行をする必要がある。

【特許文献１】 特許第２０８６９２４号公報

【発明の開示】

【発明が解決しようとする課題】

【０００５】

上述したように、従来の技術では、外部アプリケーションがカード内のデータおよび、データの暗号化情報を一旦カード外部へ読み出し、データ交換可否を決定し、演算や書き込みの処理を行うため、暗号化情報が外部に漏洩する危険性があり、さらに電子マネーなどの重要なデータも外部に漏洩、改竄される危険が発生するという課題を有していた。

本発明は、前記従来の課題を解決するもので、ＩＣカードに代表される半導体メモリカードに格納されている異なるサービス間のデータのセキュリティを保ったまま、カード内部でデータのコピーや移動等の処理を行うこと可能にすることにより、電子マネーや個人情報などの重要なデータが外部に漏洩することを防止することが可能な半導体メモリカードを提供することを目的とする。

【課題を解決するための手段】

【０００６】

前記従来の課題を解決するために、本発明の半導体メモリカードは、複数のサービスを提供可能な半導体メモリカードにおいて、複数のサービス間に共通であり、各サービスのセキュリティレベルを定義したセキュリティレベル情報を設定管理するセキュリティレベル管理手段と、前記セキュリティレベル情報を取得するセキュリティレベル情報取得手段を備えた。

さらに、本発明の半導体メモリカードでは、前記セキュリティレベル情報取得手段により取得した前記セキュリティレベル情報を出力するセキュリティレベル情報出力手段とを備えた。

さらに、本発明の半導体メモリカードでは、前記セキュリティレベル情報取得手段で取得した前記セキュリティレベル情報を比較し、前記セキュリティレベル情報比較手段で比較した結果により所定のデータ操作処理を行うデータ操作手段を備えた。

また、さらに本発明の半導体メモリカードでは、前記セキュリティレベル情報は、各サービスにおいて取り扱うデータの暗号化条件とした。

また、さらに本発明の半導体メモリカードでは、前記セキュリティレベル情報は、前記サービスを提供するアプリケーションのバージョン番号を含むようにした。

また、さらに本発明の半導体メモリカードでは、前記セキュリティレベル情報比較手段は、比較結果を保存し、該保存した比較結果を参照してセキュリティレベル情報を比較する。

【０００７】

また、本発明の半導体メモリカード処理方法は、複数のサービス間に共通であり、各サービスのセキュリティレベルを定義したセキュリティレベル情報を設定管理し、前記セキュリティレベル情報を取得することを特徴とする。

また、本発明の半導体メモリカード処理プログラムは、複数のサービス間に共通であり、各サービスのセキュリティレベルを定義したセキュリティレベル情報を設定管理し、前記セキュリティレベル情報を取得することを特徴とする。

また、本発明の集積回路は、複数のサービス間に共通であり、各サービスのセキュリティレベルを定義したセキュリティレベル情報を設定管理するセキュリティレベル情報管理手段と、前記セキュリティレベル情報を取得するセキュリティレベル情報取得手段とを備えること特徴とする。

【発明の効果】

【０００８】

以上説明したように、複数のサービス間に共通のセキュリティレベル情報と、セキュリティレベル情報を取得するセキュリティレベル情報取得手段とを備えることで、複数のサービスを提供可能な半導体メモリカードを扱う上で、複数サービス間のデータ交換可否を容易に決定することができる。

また、取得したセキュリティレベル情報を出力するセキュリティレベル情報出力手段とを備える構成により、外部ホストにより、複数サービス間のデータ交換可否を容易に決定することができる。

また、取得したセキュリティレベル情報を比較するセキュリティレベル情報比較手段と、比較した結果によりデータ操作処理を行うデータ操作手段を備える構成により、半導体メモリカード内部でデータ処理を完結できるのでセキュリティ機能が高く、ユーザは安心して利用することが可能となる。

また、セキュリティレベル情報を、取り扱うデータの暗号化条件とすることで、データを交換する対象となるサービスもしくは、アプリケーションに対する暗号強度を参照し、暗号強度のより高いサービスもしくは、アプリケーションへのデータ移動は許可し、暗号強度の低いサービスもしくは、アプリケーションへのデータ移動は禁止することにより、データの秘匿性を維持したままデータ交換が可能となる。その結果、ユーザは安心して半導体メモリカードを利用することが可能となる。

また、セキュリティレベル情報にアプリケーションのバージョン番号を含むことで、アプリケーションのアップデートなどの更新情報が反映され、さらにセキュリティ機能を高くすることが可能となる。

また、セキュリティレベル情報比較手段で比較した結果を保存し、保存されている比較結果を参照し、比較することで、認証時間の短縮を図ることができ、ユーザは快適に半導体メモリカードを利用することが可能となる。

#### 【発明を実施するための最良の形態】

##### 【0009】

以降、本発明にかかる半導体メモリカードの実施形態について説明する。本実施形態にかかる半導体メモリカードは、耐タンパモジュールを内蔵したICカードである。以下本発明の実施の形態について、図面を参照しながら説明する。

##### 【0010】

###### （実施の形態1）

まず始めに、本発明に係るICカードの実施行為のうち、使用行為について説明する。ICカード200は単体、及びポータブルデバイス122と接続され、図1に示すような環境でユーザの利用に供される。図1はICカードの使用環境を示す図である。図1における使用環境は、ECサーバ100、公共サービスサーバ110、無線基地局120、カードリーダーライタ121、ポータブルデバイス122、ネットワーク123から構成される。

##### 【0011】

ECサーバ100及び公共サービスサーバ110は、無線基地局120及びカードリーダーライタ121、ネットワーク123を介してICカード200にECサービス及び公共サービスを提供する。ECサーバ100及び公共サービスサーバ110には複数のECアプリケーションプログラム（101～104）及び公共アプリケーションプログラム（111～113）が動作しており、これらのそれぞれは固有のECサービス及び公共サービスをICカード200に提供する。ECサーバ100上で動作するECアプリケーションは、サーバアプリケーションであり、ECサービスの種類毎にそれぞれ異なるものが存在する。

図1では、n種のECサービス毎のECアプリケーションをE-APL1、2、・・・i、nと略記している。また公共サービスサーバ110上で動作する公共アプリケーションもサーバアプリケーションであり、公共サービスの種類毎にそれぞれ異なるものが存在する。図1では、n種の公共サービス毎の公共アプリケーションをP-APL1、・・・i、nと略記している。

カードリーダーライタ121は、具体的にはクレジット会社などのキャッシュディスベンサーであり、ICカード200との入出力を行う。カードリーダーライタ121はネットワーク123と接続されており、このカードリーダーライタ121を介することでICカード200は、ECサーバ100のECサービス及び公共サービスサーバ110の公共サービスを受けることが可能である。

##### 【0012】

無線基地局120は建物や電柱の屋上に備え付けの機器であり携帯電話型のポータブル

・ノバ11へ122と無線によるノード間の通信を行う。無線基地局120はノード122と接続されており、この無線基地局120を介することでもポータブルデバイス122はECサーバ100のECサービス及び公共サービスサーバ110の公共サービスを受けることが可能である。

ポータブルデバイス122はICカード200を接続してICカード200にアクセスする機器である。ポータブルデバイス122にはブラウザソフトなどがインストールされており、ユーザはこのブラウザのユーザインタフェースを介して、ICカード200内のデータにアクセスすることができる。

#### 【0013】

図2は、一般的なICカード200のハードウェア構成を示す図である。図2に示すようにICカードにはCPU201、RAM202、ROM203、EEPROM204、IF205が実装されており、マイコンシステムを形成している。

次にマルチアプリケーション対応のICカードにおけるデータ操作について説明する。図4は、一般的なICカードとホストにおけるデータ操作の概略図である。各アプリケーション単体でのデータ処理は、カードリーダーライタ121を介して、サーバアプリケーションが行う。カードリーダーライタ121はポータブルデバイス122、基地局120であってもよい。

#### 【0014】

ここでICカード内クライアントECアプリケーションであるC-E-APL1(301)のデータを別のICカード内クライアントECアプリケーションであるC-E-APL2(302)にコピーあるいは移動する場合について説明する。

まず、サーバ100内のECサーバアプリケーションE-APLi(103)がE-APL1(101)とICカード内クライアントECアプリケーションC-E-APL1(301)の認証を行い、次にE-APL2(102)とC-E-APL2(302)の認証を行う。認証処理完了後、E-APLi(103)はE-APL1(101)にデータの読み出しを要求し、カードリーダーライタ121を介してE-APL1(101)がICカード200内の対応するクライアントECアプリケーションC-E-APL1(301)のデータ331を読み出す。次に、E-APLi(103)はE-APL2(102)にデータの書き込みを要求し、カードリーダーライタ121を介してE-APL2(102)がICカード200内の対応するクライアントECアプリケーションC-E-APL2(302)にデータ332を書き込む。

従って、ICカード内の実データはポータブルデバイスの外へ出る。これは、ICカード内のOSにより各アプリケーション用メモリ領域がファイヤウォール340で保護されているためである。

#### 【0015】

次に、本発明のICカードについて説明する。図5は本発明におけるICカードにおけるデータ操作の概略図である。本発明のICカードは、各アプリケーション単体でのデータ処理は一般的なICカードの処理と変わらない(図4参照)。また、カードのハードウェア構成は一般的なICカードのハードウェア構成(図2)と変わらない。

図6は本発明の基本となるマルチアプリケーション対応のICカードのソフトウェア構成を示した図である。アプリケーション用メモリ領域310、OS311、クライアントECアプリケーション301と、クライアントECアプリケーション302、とを備えている点は一般的なICカードと変わらない。

しかし、本発明では複数のサービス間に共通であり、各サービスのセキュリティレベルを定義したセキュリティレベル定義情報600と、ICカード内に格納されているアプリケーションを管理するためのアプリケーション情報管理テーブル601と、前記セキュリティレベル情報とアプリケーション情報管理テーブルを管理するセキュリティレベル情報管理手段602と、前記セキュリティレベル情報を取得するセキュリティレベル情報取得手段604と、前記セキュリティレベル情報取得手段により取得した前記セキュリティレベル情報を出力するセキュリティレベル情報出力手段605と、前記セキュリティレベル

・情報出力手段により出力されたセキュリティレベル情報をサーバ側で比較するサーバ側セキュリティレベル情報比較手段607と、前記セキュリティレベル情報出力手段により出力されたセキュリティレベル情報をカード内で比較するクライアント側セキュリティレベル情報比較手段606と、前記セキュリティレベル情報比較手段で比較した結果を基に、所定のデータ操作処理を行うデータ操作手段608、とを備えている点が異なる。

#### 【0016】

セキュリティレベル定義情報600は、セキュリティレベルの高低により異なる条件を含む(図7)。例えば、値が03hの場合はセキュリティレベルが“高”であり、データをTriple-DES方式で暗号化する。次に値が02hの場合はセキュリティレベルが“中”であり、データをDES方式で暗号化する。さらに値が01hの場合はセキュリティレベルが“低”であり、データをAES方式で暗号化する。値が00hの場合はセキュリティレベルが“なし”であり、データを暗号化しない、という条件である。

アプリケーション情報管理テーブル601は、ICカード内に格納されている各アプリケーションに関する情報を保持している(図8)。アプリケーションに関する情報とは、例えば、アプリケーションを識別するためのアプリケーションID、前記セキュリティレベル定義情報600で定義されたセキュリティレベル、暗号鍵のビット長である暗号情報、暗号鍵、アプリケーションのバージョン情報などである。図8では、クライアントECアプリケーションC-E-APL1(301)は、アプリケーションIDが3412h、セキュリティレベルが01h(低)、暗号鍵ビット長が80h、暗号鍵が128bit(16byte)分、バージョン情報が01hであることを示しており、クライアントECアプリケーションC-E-APL2(302)は、アプリケーションIDが7856h、セキュリティレベルが03h(高)、暗号鍵ビット長がC0h、暗号鍵が192bit(24byte)分、バージョン情報が05hであることを示しており、クライアント公共アプリケーションC-P-APL1(303)は、アプリケーションIDがFFFEh、セキュリティレベルが02h(中)、暗号鍵ビット長が40h、暗号鍵が64bit(8byte)分、バージョン情報が1Ahであることを示している。

#### 【0017】

以下、図9において、データ操作要求において操作が完了するまでの手順を示すフローチャートを参照し、本発明のICカードの動作について詳細に説明を行う。

まず、処理要求発生後ECサーバ100のサーバアプリケーションE-APLi(103)はサーバアプリケーションE-APL1(101)の認証をICカード内のクライアントECアプリケーションC-E-APL1(301)に対して行い(S901)、次にE-APL1(101)に対応するE-APL2(102)の認証もクライアントECアプリケーションC-E-APL2(302)に対して行う(S902)。各アプリケーション認証完了後、ユーザはデータ操作したいデータを選択する(S903)。

その後、セキュリティレベル情報取得手段604はアプリケーションIDを元に、セキュリティレベル情報管理手段602からクライアントECアプリケーションC-E-APL1(301)及びC-E-APL2(302)のセキュリティレベル情報を取得する(S904)。次に、セキュリティレベル情報出力手段605は取得したセキュリティレベル情報を出力し(S905)、ICカード200はECサーバ100に対して、セキュリティレベル情報を含むレスポンスを返す。さらに、ECサーバ100内のサーバ側セキュリティレベル情報比較手段607は、出力されたセキュリティレベル情報を比較し、条件を満たす場合は、ICカード200にデータ操作をICカード内部で実行するよう要求(APDUコマンド)を送信する(S906)。そして、ICカード200ではデータ操作手段608は出された要求やアプリケーションID、ファイルIDなどのデータ操作情報を元に、選択されたC-E-APL1(301)のデータをC-E-APL2(302)にコピーする処理を実行する(S907)。

ここで、条件を満たさない場合はICカード外部つまりECサーバ100を介して操作を実行することをユーザに確認し(S909)、処理続行であれば、サーバを介して処理を実行する(S910)。処理完了後、処理を続行する場合は、処理データの選択(S9



・ ヴィジに成るこくする。

#### 【0018】

具体的に、ユーザがクライアントECアプリケーションC-E-APL1(301)に格納されている氏名、住所、電話番号などの個人情報をクライアントECアプリケーションC-E-APL2(302)にコピーしたい場合についての例を示す。

ユーザはポータブルデバイス122やカードリーダーライター121等の表示画面でC-E-APL1(301)及びC-E-APL2(302)を選択する。これによりICカード200は各アプリケーションの認証を実行する(S901、S902)。その後、表示画面でコピー処理を実行したいデータ(ここでは、氏名、住所、電話番号とする)の選択を行う(S903)。データ選択完了後ICカード200では、セキュリティレベル情報取得手段604を用いて、指定された各アプリケーションのセキュリティレベル情報を取得し(S904)、取得したセキュリティレベル情報をECサーバ100にレスポンスとして送信する(S905)。ECサーバ100は出力されたセキュリティレベル情報を元に各サービスのレベルの比較を行う。ここで、C-E-APL1(301)のセキュリティレベル情報は値が01hであるため、レベル“低”であり、C-E-APL2(302)のセキュリティレベルは値が03hであるためレベル“高”となる。従って、コピー元(C-E-APL1(301))のセキュリティレベルのほうが低レベルであるため、ICカード200にカード内で処理を行うよう要求し、セキュリティレベルが“低”であるC-E-APL1(301)から、セキュリティレベルが“高”であるC-E-APL2(302)へ、カード内でのコピー処理が可能となる(S907)。コピー処理完了後、表示画面に処理を続行するかどうかの選択画面が現れるため、ユーザは他のデータのコピーを実行したいのであれば、他のデータを選択することが可能となる。

#### 【0019】

以上、セキュリティレベルが“低”であるようなアプリケーションから、セキュリティレベルが“高”であるようなアプリケーションに対するデータコピーないし移動は、特別な指示がなくても可能であるが、逆に、セキュリティレベルが“高”であるようなアプリケーションから、セキュリティレベルが“低”であるようなアプリケーションに対するデータコピーないし移動は、データの秘匿性の維持の観点からユーザに対する警告を行ってデータコピーないし移動をするか、それを禁止することが望ましい。かかる構成によれば、各サービスに共通のセキュリティレベル定義情報を持ち、各サービスのセキュリティレベル情報を取得し、取得したセキュリティレベル情報を出力し、出力されたセキュリティレベル情報をサーバで比較し、条件を満たす場合はカード内部でデータ操作を行うことが可能となり、利用者はデータが外部に漏洩する危険性を有することなく異なるサービス間のデータ操作を完了することができる。

#### 【0020】

##### (実施の形態2)

第1の実施形態では、セキュリティレベル情報の比較をサーバアプリケーションであるE-APLi(103)で行っていたが、本発明はこれに限定されるものではなく、ICカード内部で比較する場合も考えられる。そこで、第2実施形態では、ICカード内にクライアント側セキュリティレベル情報比較手段606を備えた場合を示すこととする。

図10のフローチャートを参照し、本発明のICカードの動作について説明を行う。基本的な処理の流れは、第1実施形態と変わらない。しかし、クライアント側セキュリティレベル情報比較手段606をICカード内部に備えることで、取得したセキュリティレベル情報を外部に出すことなく比較する(S1005)ことが可能となる点が異なる。

また、第1実施形態では、セキュリティレベル情報を“高”、“中”、“低”、“なし”、としていたが、第2実施形態ではセキュリティレベル情報を、各サービスの実データ等を暗号化するための暗号化条件、例えば、鍵長、鍵データ、暗号化方式とすることも特徴とする。

この場合、セキュリティレベル情報の比較をサーバで行うと、各アプリケーションに対応する暗号化条件が外部に漏洩し、実データが改ざんされる可能性があるため、第2実施

・形態を取ることで、半女はノードの構成を閉、ことが可能となる。

#### 【0021】

##### （実施の形態3）

第2の実施形態では、セキュリティレベル情報を各サービスの実データ等を暗号化するための暗号化条件としていたが、第3実施形態では、セキュリティレベル情報にはアプリケーションプロトコルのバージョンを含むことも特徴とする。

従来、ICカード200とサーバ100、110（カードリーダー121）では図11に示すアプリケーションプロトコルデータユニット（APDU）コマンドを使用してデータの送受信が行われている。そこで、APDUコマンドのヘッダ部分である制御パラメータ（P1、P2）を用いてアプリケーションプロトコルバージョンをコマンドに付加することも特徴とする。

一般に、アプリケーションプロトコルは機能拡張されるにしたがってその、バージョン番号を上げて定義される。例えば、セキュリティ上の拡張または、改良を加えた結果バージョン番号が上ることがある。その場合、プロトコルバージョンを比較して、より上位バージョンのプロトコルの方がセキュリティ強度が高いといえる。

#### 【0022】

以下、図12以降の図を用いて、APDUコマンドにアプリケーションプロトコルバージョンを付加する場合について説明する。

図12はISO7816で規定されており、金融系で使用されているコマンドを示している。例えば図13に示すようにSELECTコマンドの場合、P1に未使用ビットが存在する（b8～b4）。この未使用の5ビットを用いることで、0から31までの値が設定可能となる。

また、図14に示すようにクラスバイト（CLA）のb8を1に設定することで固有コマンドが使用可能となるが、これを用いることでP1の1バイトを全てプロトコルバージョンに割り当てることも可能となり、この場合0から65535までの値が設定可能となる。

例えば、C-E-APL1（301）からC-E-APL2（302）にデータをコピーしたい場合、C-E-APL1（301）のプロトコルバージョンは01hであり、C-E-APL2（302）のプロトコルバージョンは05hであるため、比較結果C-E-APL2（302）のプロトコルバージョンが上位であり、セキュリティ強度が高いと判断できるため、データコピー処理の実行が可能となる。

以上説明したように、APDUコマンドにアプリケーションプロトコルバージョンを付加することで、アプリケーションごとのプロトコルバージョンを取得し、比較することが可能となり、コピー先のアプリケーションプロトコルバージョンがコピー元のアプリケーションプロトコルバージョンより古いバージョンの場合は、通信セキュリティレベルが落ちると判断しデータコピーなどの処理を不可とすることが可能となり、データ漏洩の危険性が減少することとなる。

#### 【0023】

##### （実施の形態4）

さらに、第1の実施形態において、サーバ内のアプリケーションで、出力されたセキュリティレベル情報を比較していたが、本発明はこれに限定されるものではなく、比較した結果を保存しておく場合も考えられる。この場合、同一アプリケーション間での認証、及び比較をデータ操作の度に行う必要が無く、処理時間の短縮が図られることとなる。

#### 【0024】

##### （実施の形態1～実施の形態4の第1の補足事項）

以上、実施形態1、2、3、4を説明した。尚、これまでの説明において本発明のICカードにおいて備えている、セキュリティレベル情報管理手段、セキュリティレベル情報取得手段、セキュリティレベル情報出力手段、セキュリティレベル情報比較手段、データ操作手段等は、コンピュータプログラムとして実現される。当該プログラムは、ICカード内のROMに格納され実行されるものと、外部よりダウンロードされ、不揮発性メモリ

・に包摂されたりされるものがある。

#### 【0025】

（実施の形態1～実施の形態4の第2の補足事項）

また、さらに、上述の機能ブロックは、CPU、RAM、ROM、不揮発性メモリ等のハードウェア資源との組み合わせにより、集積回路であるLSIとして実現される場合がある。これらは、個別に1チップ化されても良いし、一部又はすべてを含むように1チップ化されても良い。

図15に実施の形態1、実施の形態2、実施の形態3における集積回路化の一例を示す。LSI2000は集積回路化の一例を示し、集積回路化する機能ブロックの範囲の例である。ここでは、LSIとしたが、集積度の違いにより、IC、システムLSI、スーパーLSI、ウルトラLSIと呼称されることもある。

また、集積回路化の手法はLSIに限るものではなく、専用回路又は汎用プロセッサで実現してもよい。LSI製作後にプログラムすることが可能なFPGA(Field Programmable Gate Array)やLSI内部の回路セルの接続や設定を再構成可能なリコンフィギュラブル・プロセッサを利用してても良い。

さらには、半導体技術の進歩又は派生する別技術によりLSIに置き換わる集積回路化の技術が登場すれば、当然その技術を用いて機能ブロックの集積化を行ってもよい。バイオ技術の適用等が可能性としてありえる。

#### 【産業上の利用可能性】

#### 【0026】

本発明にかかる半導体メモリカードは、カード内のアプリケーションのみでデータ交換が可能であるため、複数のサービスを提供可能かつデータの保護機能に優れた半導体メモリカード等として有用である。

#### 【図面の簡単な説明】

#### 【0027】

【図1】一般的なICカードの利用形態概観図

【図2】一般的なICカードのハードウェア構成図

【図3】一般的な複数サービス対応のICカードのソフトウェア構成図

【図4】一般的な複数サービス対応ICカードのデータ処理（コピー、移動）概略図

【図5】本発明の基本となる複数サービス対応ICカードのデータ処理（コピー、移動）概略図

【図6】本発明のソフトウェア構成図

【図7】セキュリティレベル定義情報構成図

【図8】アプリケーション情報管理テーブル構成図

【図9】本発明のデータ処理手順フローチャート1

【図10】本発明のデータ処理手順フローチャート2

【図11】アプリケーションプロトコルデータユニット構成図

【図12】全産業共通コマンド例を示す図

【図13】SELECTコマンドにおける制御パラメータ1を示す図

【図14】命令クラスバイトを示す図

【図15】実施の形態1、実施の形態2、実施の形態3における集積回路化の一例を示す図

#### 【符号の説明】

#### 【0028】

100 ECサーバ

200 ICカード

301 クライアントECアプリケーション1

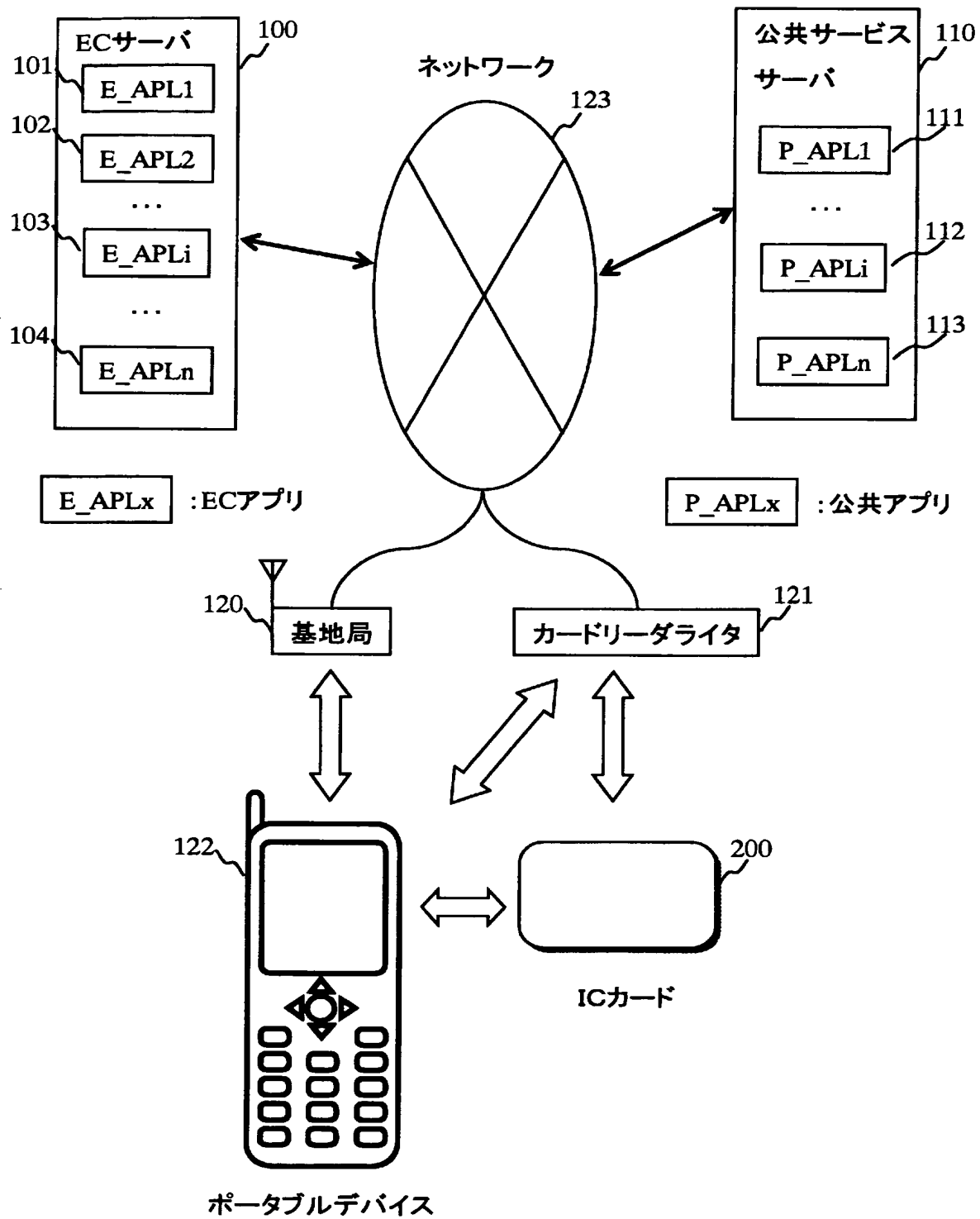
302 クライアントECアプリケーション2

310 アプリケーション用メモリ領域

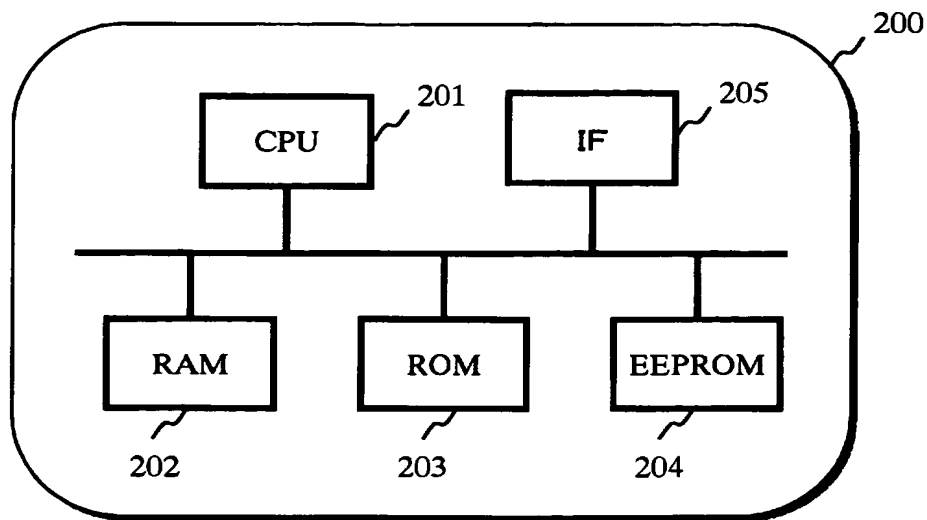
331 アプリケーション1内データ領域（複写元）

- ・ 5 5 2 ノノリノーションコンメンノノ領域（概ナリノ）
- 6 0 0 セキュリティレベル定義
- ・ 6 0 1 アプリケーション情報管理テーブル
- 6 0 2 セキュリティレベル情報管理手段
- 6 0 3 セキュリティレベル情報設定手段
- 6 0 4 セキュリティレベル情報取得手段
- 6 0 5 セキュリティレベル情報出力手段
- 6 0 6 クライアント側セキュリティレベル情報比較手段
- 6 0 7 サーバ側セキュリティレベル情報比較手段
- 6 0 8 データ操作手段

【 図 1 】

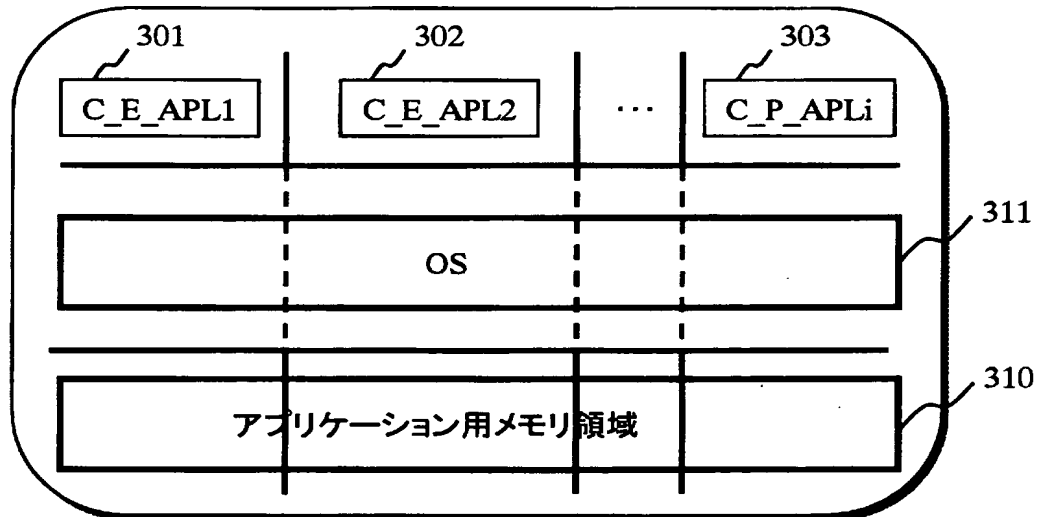


ICカード

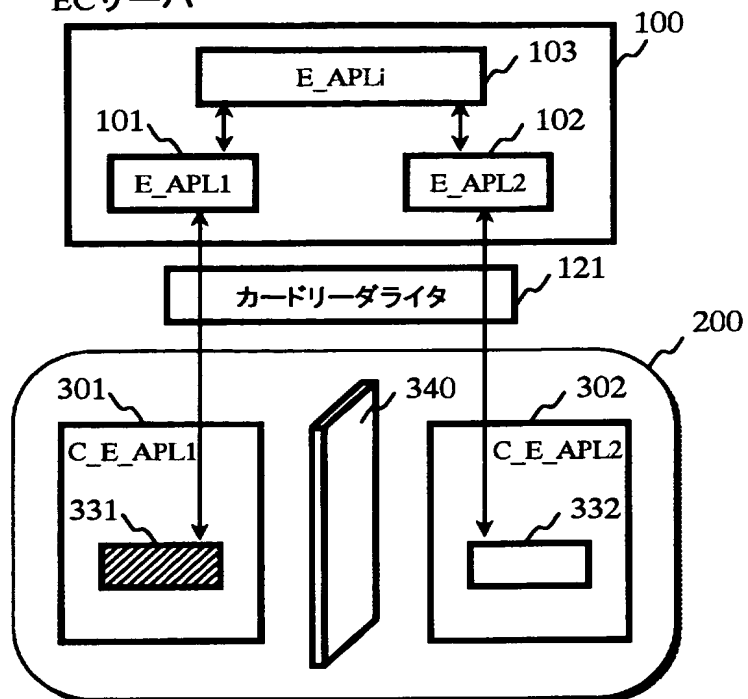


【図 3】

アプリケーション間ファイヤウォール機能

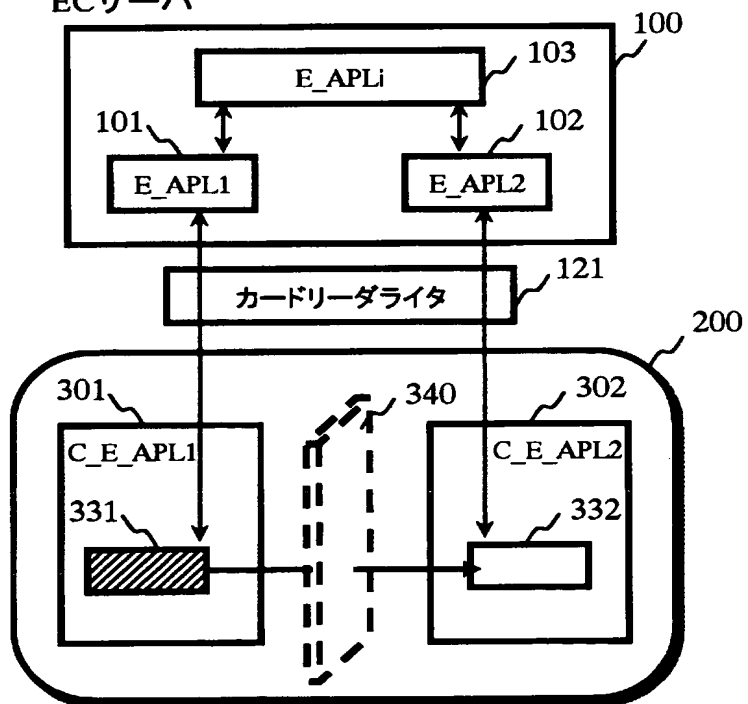


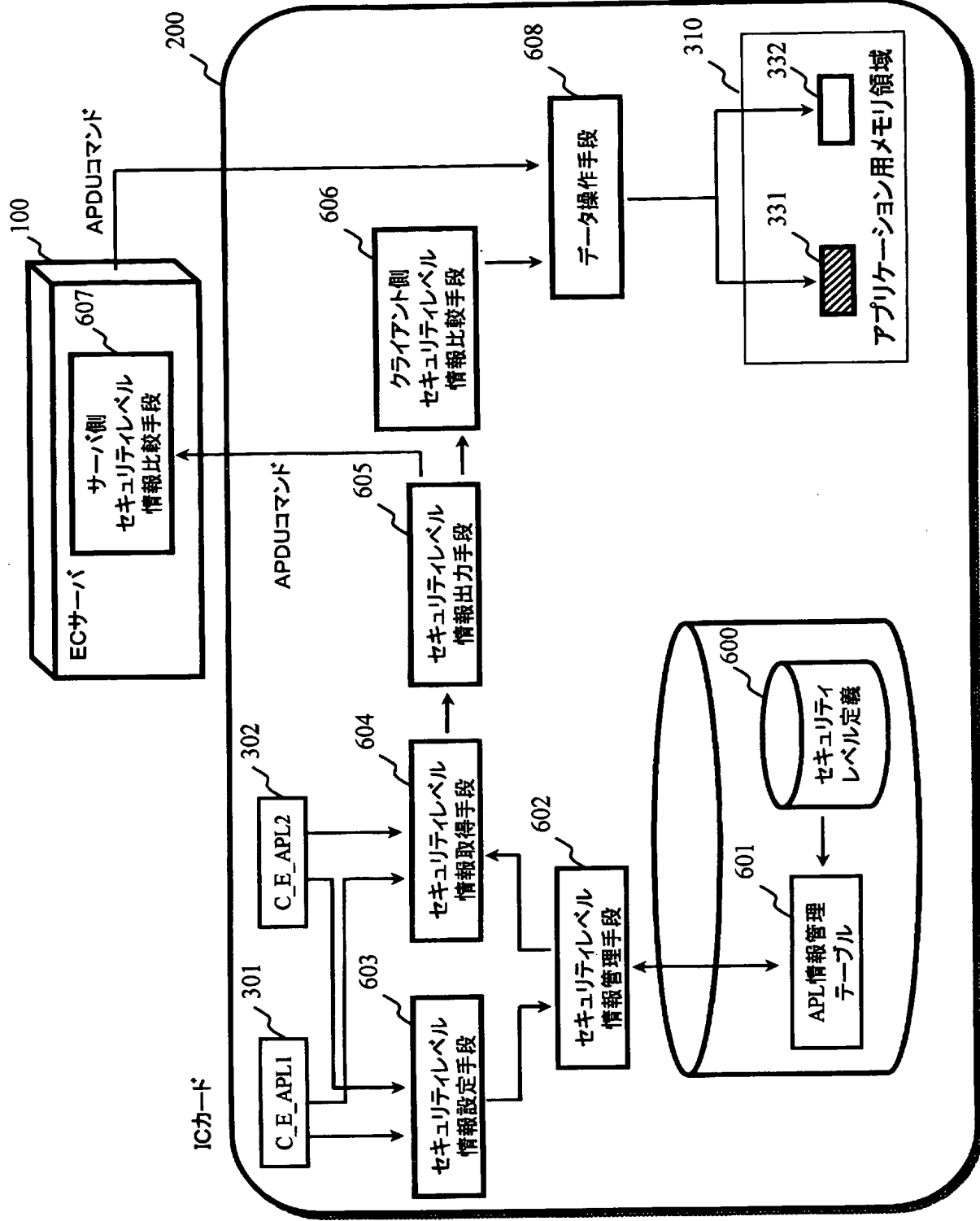
ECサーバ



【図 5】

ECサーバ



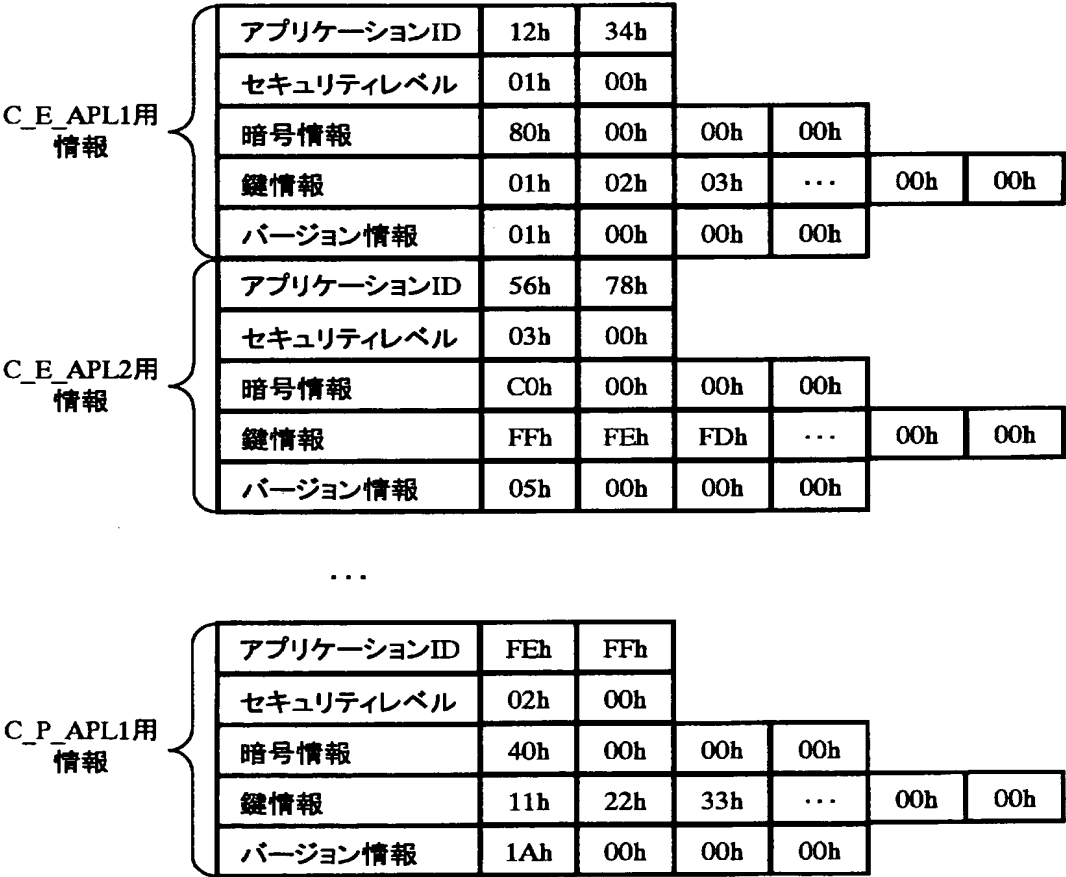
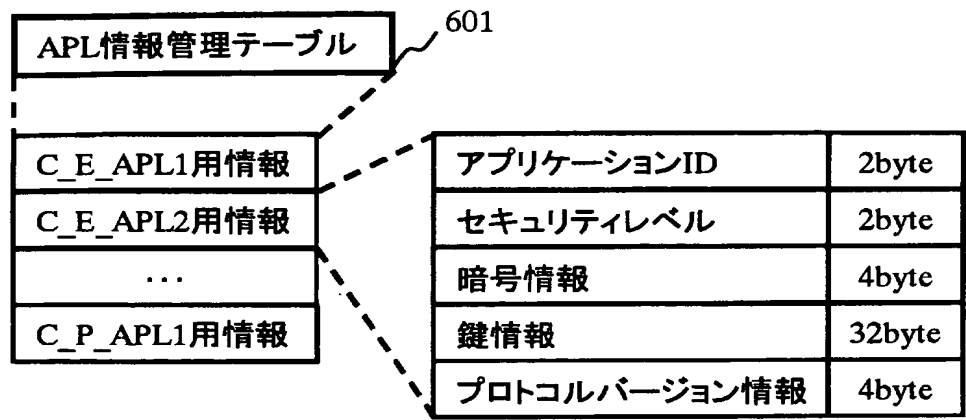


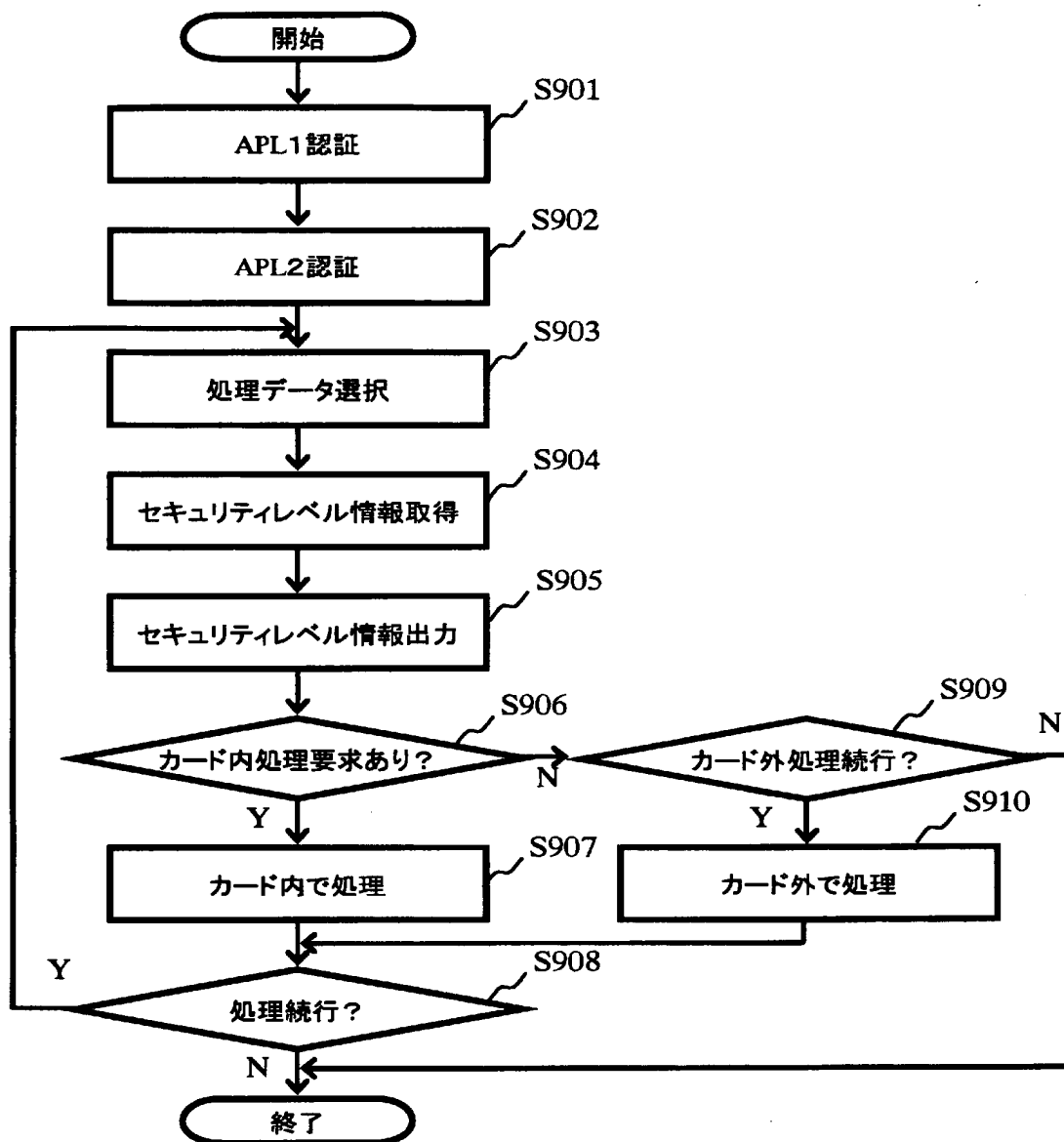


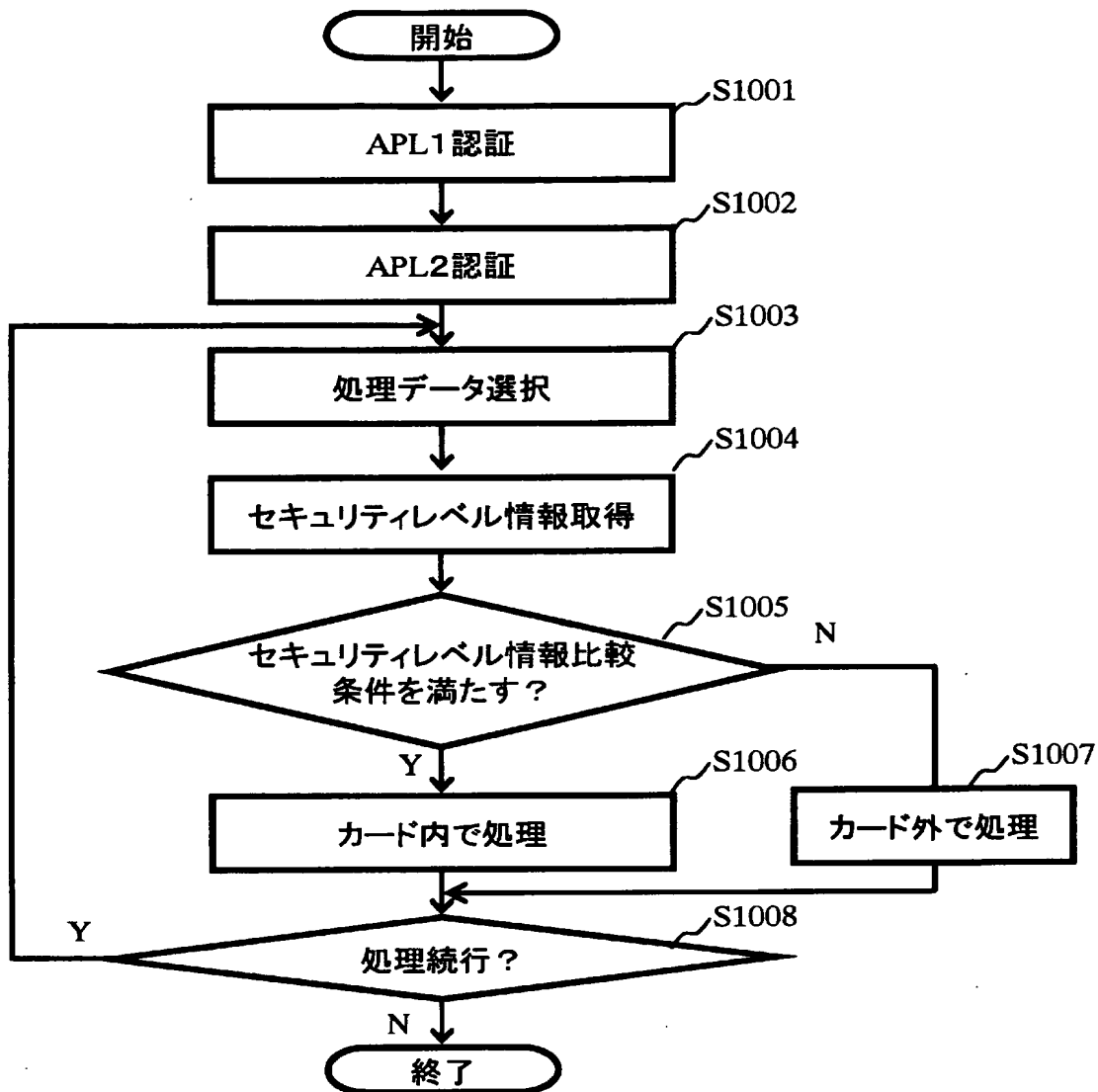


700

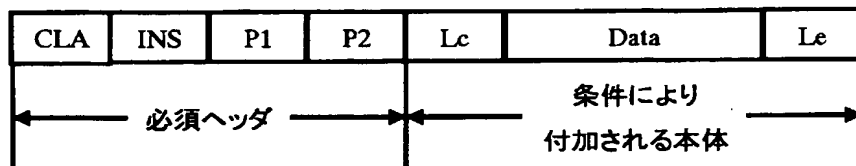
レベル	値	レベルの基準
高	03h	Triple-DES暗号方式
中	02h	DES暗号方式
低	01h	AES暗号方式
なし	00h	暗号なし







【図 11】



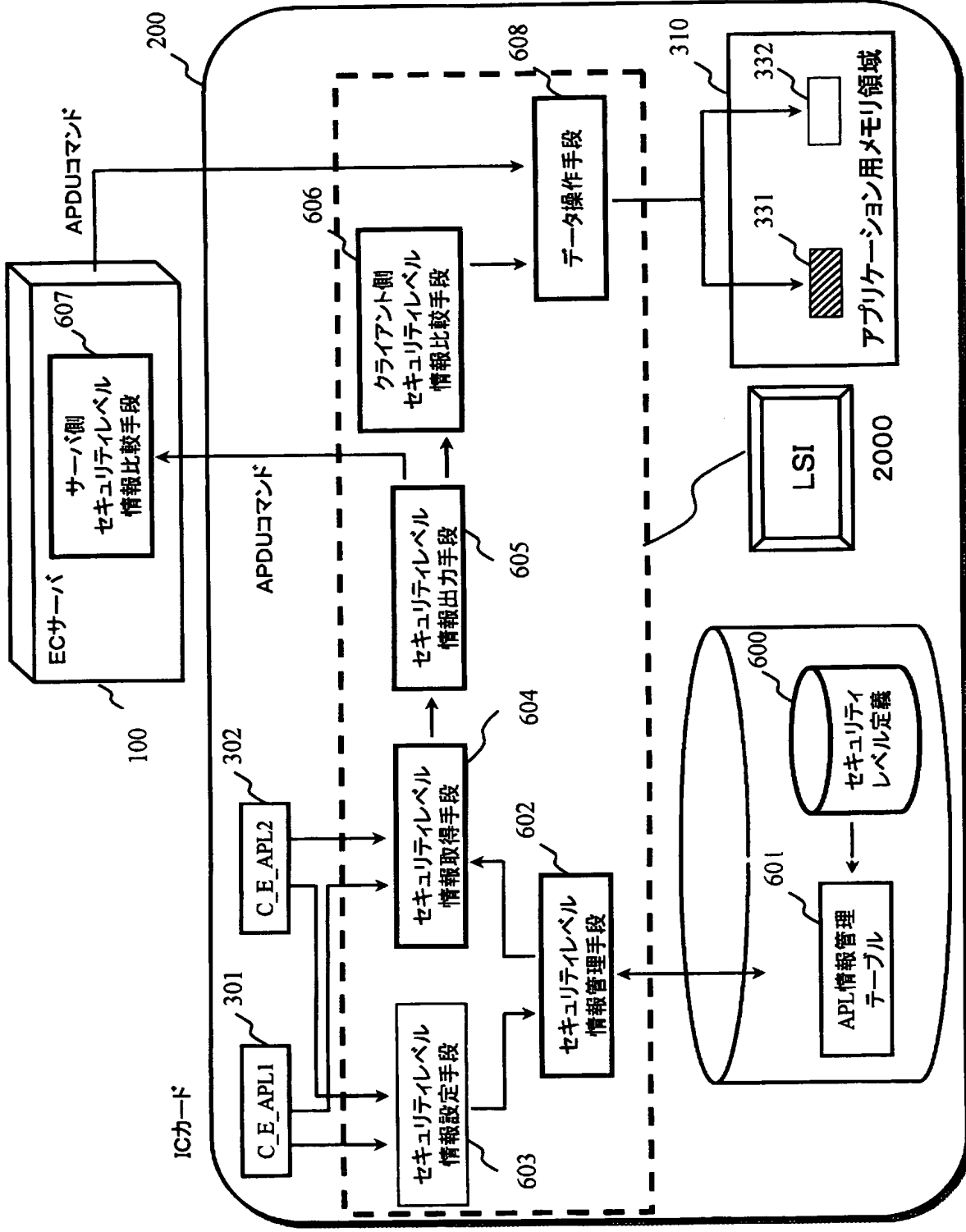
コマンド名	SELECT	READ RECORD	INTERNAL AUTHENTICATE
CLA(1byte)	00h	00h	00h
INS(1byte)	A4h	B2	88h
P1(1byte)	XXh	レコード番号	00h
P2(1byte)	00h	XXh	00h

【図 1 3】

b8	b7	b6	b5	b4	b3	b2	b1	意味
x	x	x	x	x				未使用
					1			名前による選択
						0	0	

【図 1 4】

b8	b7	b6	b5	b4	b3	b2	b1	意味
0	0	0	0					全産業共通コマンド
1	0	0	0					独自コマンド



【要約】

【課題】 I C カード内のデータをカード外部に読み出すことなくデータ交換を行うことが可能な I C カードを提供すること。

【解決手段】 セキュリティレベル定義情報 6 0 0 と、アプリケーション情報管理テーブル 6 0 1 と、セキュリティレベル情報管理手段 6 0 2 と、セキュリティレベル情報取得手段 6 0 4 と、セキュリティレベル情報出力手段 6 0 5 と、クライアント側セキュリティレベル情報比較手段 6 0 6 と、データ操作手段 6 0 8、とを備え、 I C カード内でデータ操作が完結するため、ユーザは個人情報などの重要なデータが外部に漏洩する危険性を有することなく I C カードを利用することが可能となる。

【選択図】 図 6

0 0 0 0 0 5 8 2 1

19900828

新規登録

大阪府門真市大字門真 1 0 0 6 番地

松下電器産業株式会社



# Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/JP05/006805

International filing date: 31 March 2005 (31.03.2005)

Document type: Certified copy of priority document

Document details: Country/Office: JP  
Number: 2004-114330  
Filing date: 08 April 2004 (08.04.2004)

Date of receipt at the International Bureau: 12 May 2005 (12.05.2005)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b)



World Intellectual Property Organization (WIPO) - Geneva, Switzerland  
Organisation Mondiale de la Propriété Intellectuelle (OMPI) - Genève, Suisse

**This Page is Inserted by IFW Indexing and Scanning  
Operations and is not part of the Official Record.**

## **BEST AVAILABLE IMAGES**

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

☒ **BLACK BORDERS**

☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**

☐ **FADED TEXT OR DRAWING**

☐ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**

☐ **SKEWED/SLANTED IMAGES**

☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**

☐ **GRAY SCALE DOCUMENTS**

☒ **LINES OR MARKS ON ORIGINAL DOCUMENT**

☒ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**

☐ **OTHER:** \_\_\_\_\_

**IMAGES ARE BEST AVAILABLE COPY.**

**As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.**